UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/559,259	04/27/2000	Hideyuki Hirano	1405.1020	2237

21171 7590 03/14/2005

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
REAGAN, JAMES A	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 03/14/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)	
Office Action Summary	09/559,259	HIRANO ET AL.	
	Examiner	**Art Unit**	
	James A. Reagan	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 December 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-26* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-26* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

1. This action is in response to the amendment received on 16 December 2004.

2. Claims 1-26 have been amended.

3. Claims 1-26 have been examined.

4. The rejections of claims 1-26 have been updated to reflect the amended limitations.

RESPONSE TO ARGUMENTS

5. Applicant's arguments received on 16 December 2004 have been fully considered but they are not persuasive. Referring to the previous Office action, Examiner has cited relevant portions of the references as a means to illustrate the systems as taught by the prior art. As a means of providing further clarification as to what is taught by the references used in the first Office action, Examiner has expanded the teachings for comprehensibility while maintaining the same grounds of rejection of the claims, except as noted above in the section labeled "Status of Claims." This information is intended to assist in illuminating the teachings of the references while providing evidence that establishes further support for the rejections of the claims.

Applicant's arguments with respect to claims 1-26 have been considered but are moot in view of the new ground(s) of rejection.

With regard to claims 10-15 and 18-21, the common knowledge declared to be well-known in the art is hereby taken to be admitted prior art because the Applicant either failed to traverse the Examiner's assertion of Official Notice or failed to traverse the Examiner's assertion of Official Notice adequately. To adequately traverse the examiner's assertion of Official Notice, the Applicant must specifically point out the supposed errors in the Examiner's action, which

would include stating why the noticed fact is not considered to be common knowledge or well-known in the art. A general allegation that the claims define a patentable invention without any reference to the Examiner's assertion of Official Notice would be inadequate. Support for the Applicant's assertion of should be included.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-6, and 16-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yasukawa et al. (US 5,999,622) in view of Rhoads (US 6,343,138), in view of Millsted et al. (US 6,263,313 B1), and further in view of Stefik et al. (US 6,233,684 B1).

Examiner's note: Examiner has pointed out particular references contained in the prior art of record in the body of this action for the convenience of the Applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply. Applicant, in preparing the response, should consider fully the *entire* reference as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Claims 1, 25, and 26:

With regard to the limitation of:

- *preparing a substantive file by encrypting digital content file,* Yasukawa discloses distribution of encrypted data (column 1, lines 21-27).

- *synthesizing the substantive file and the user-specific-authorization-information-embedded preview sample to prepare a synthesized digital content file,* Yasukawa discloses combining encrypted and non-encrypted data into a single file (column 3, lines 65-67).

Yasukawa does not specifically disclose *extracting, as a preview sample, a portion of a digital content file to be distributed,* and *embedding user-specific authorization information containing information for accessing the encrypted digital content file, as invisible information in the extracted preview sample to prepare user-specific-authorization-information-embedded preview sample data.* However, in column 3, lines 39-52, Yasukawa discloses encrypting only some segments of the complete file. In column 4, lines 16-20, Yasukawa discloses encrypted and non-encrypted parts. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the invention of Yasukawa to encrypt just a sample of the data file and reinsert the encrypted section into the data file because it allows digital information to be copied and distributed easily over a wide variety of mediums, including modems, wireless technologies, CD-ROMs, floppy disks, the Internet, bulletin boards, computer networks etc., while preventing unauthorized use of the data.

In addition, Yasukawa does not specifically disclose the use of invisible or hidden data. Rhoads, however, does show an identification code signal is hidden in a carrier signal (abstract). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the encryption method of Yasukawa with Rhoads' use of hidden data because if a given entity can recognize the signatures hidden within a given set of empirical data, that same entity can take steps to remove those signatures (Rhoads, column 63, lines 3-5).

The combination of Yasukawa/Rhoads does not specifically disclose data samples for preview purposes. However, Millsted discloses digital clips (column 81, lines 45-55), data extraction and previewing (column 75, lines 9-21), watermarking (column 64, line 61 to column 65, line 18), and encryption/decryption techniques for distribution of digital works (column 2, line 52 to column 3, line 4). It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the method of Yasukawa/Rhoads' with Millsted's distribution techniques because this provides a system for tracking the use of digital data.

The combination of Yasukawa/Rhoads/Millsted does not specifically disclose embedding user-specific data. Stefik, however, in at least column 3, lines 4-55 discloses embedding a watermark in a digital file that contains rights privileges. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine the distribution techniques of Yasukawa/Rhoads/Millsted with Stefik's usage rights because it provides a system for controlling the distribution of digital works.

Claim 2:

With regard to the limitations of:

- *enabling access to the synthesized digital content file by separating the user-specific authorization information from the preview sample data unit;*
- *restoring from the user-specific authorization information a decryption key for decrypting the substantive file;*

Yasukawa discloses extracting the bitmap table from the synthesized file and decrypting the file data (column 6, line 30 to column 7, line 15).

Claim 3:

The combination of Yasukawa/Rhoads/Millsted/Stefik discloses the methods as shown above. Yasukawa/Rhoads/Millsted/Stefik do not disclose that *the preview sample is image data*

contained in the digital content file and at least one process among image processing, resizing, compressing and a γ compensation is executed on image data contained in the digital content. Rhoads, however, in column 6, line 16 to column 8, line 9 shows a process of scanning, digitizing, and processing an image to prevent unauthorized copying of the file. Rhoads also discloses scaling and resizing the image (column 8, lines 65-67), and compression and decompression techniques as well as standards (column 31, lines 26-46). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Yasukawa/Rhoads/Millsted/Stefik to use image processing techniques because this prevents the unauthorized use of image documents.

Claim 4:

With regard to the limitation of *the preview sample is index data for representing the substantive file*, Yasukawa discloses using a bitmap table as an index to identify which segments of a file have been encrypted (column 6, lines 30-34).

Claim 5:

The combination of Yasukawa/Rhoads/Millsted/Stefik discloses the methods as shown above. Yasukawa/Rhoads/Millsted/Stefik do not disclose that *the synthesized data contains a plurality of substantive data units based on a plurality of digital content items, and contains a plurality of sample data units corresponding to the plurality of substantive data units; and wherein sample data constituting the plurality of sample data units is linked with respective corresponding ones of the plurality of substantive data units.* Rhoads, however, in column 39, lines 3-12, discloses a series of frames within a movie with N-bit identification words encrypted within, wherein the plurality of frames are associated with the video stream. It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Yasukawa/Rhoads/Millsted/Stefik with Rhoads' use of multiple content items within a video

stream because this allows related content to be grouped together for ease of decryption, recognition, and use, storage, and dissemination.

Claim 6:

The combination of Yasukawa/Rhoads/Millsted/Stefik discloses the methods as shown above. Yasukawa/Rhoads/Millsted/Stefik do not disclose that *the preview sample is data structuralized in one of JPEG and MPEG formats, and the synthesized digital content file is prepared by add-on synthesizing the substantive file data unit to the preview sample using the format of the preview sample.* Rhoads, however, in column 38, lines 4-30 discloses JPEG and MPEG formats as well as inserting the digital signature into the item using the same codecs. . It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Yasukawa/Rhoads/Millsted/Stefik with Rhoads' encryption of JPEG and MPEG files because this allows the signature to be recognized and extracted using the same software that allows viewing of the JPEG or playing of the MPEG.

Claim 16:

With regard to the limitation of *the preview sample comprises as the invisible information a use count of times a user has used the digital content file; characterized in that the invisible information is rewritten each time a user uses the digital content file,* Yasukawa discloses a limited number of uses for the key (column 6, lines 18-27).

Claim 17:

With regard to the limitation of *the preview sample comprises as the invisible information authorization information to enable use count control; characterized in that the invisible information is rewritten when a user uses the digital content file a predetermined number of times and more,* Yasukawa discloses a limited number of uses for the key (column 6, lines 18-27).

Claims 18 and 20:

With regard to the limitation of *characterized in that the invisible information is rewritten on decrypting and reading the substantive file,* Yasukawa discloses various decryption key controls (column 6, lines 4-29). Yasukawa does not specifically disclose that the key use is registered as it is opened or after it is closed. However, Examiner takes **Official Notice** that it is old and well known in the encryption arts to begin the count procedure when the digital content is opened or after the user has finished viewing or using the digital content, being merely a design choice. For example, if the user is granted a duration in which to listen to a song, counting may begin as soon as the song is opened. If a user is granted permission to use shareware 10 times, counting might begin after the software is closed.

Claims 19 and 21:

With regard to the limitation of *characterized in that the invisible information is rewritten when use of the digital content file is ended.* Yasukawa discloses various decryption key controls (column 6, lines 4-29). Yasukawa does not specifically disclose that the key use is registered as it is opened or after it is closed. However, Examiner takes **Official Notice** that it is old and well known in the encryption arts to begin the count procedure when the digital content is opened or after the user has finished viewing or using the digital content, being merely a design choice. For example, if the user is granted a duration in which to listen to a song, counting may begin as soon as the song is opened. If a user is granted permission to use shareware 10 times, counting might begin after the software is closed.

Claim 22:

Yasukawa discloses the methods a shown above. Yasukawa does not specifically disclose that *the invisible information in the preview sample comprises an error recovery function by containing redundant information.* Rhoads, however, in column 7, lines 1-18 discloses an

error checking function, using 1 bit from a multi-bit word. Rhoads also discloses checksum and error-correcting codes, which ensure the exact transmission of data (column 53, lines 41-46). It would have been obvious to one of ordinary skill in the art at the time of the invention to include error-checking techniques because this ensures that data in delivered accurately.

Claim 23:

With regard to the limitation of *characterized in that limits on read-out and use in decrypting the substantive file are governed based on the invisible information in the preview sample,* Yasukawa discloses a limited number of uses for the key (column 6, lines 18-27).

Claim 24:

With regard to the limitation of *characterized in that one of year, month, date, and time limits within which read-out and use is possible in decrypting the substantive file are governed based on the invisible information in the preview sample,* Yasukawa discloses a limited number of uses for the key (column 6, lines 18-27).

8. Claims 7-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Yasukawa/Rhoads/Millsted/Stefik in view of Applicants own admission.

Claims 7 and 8:

The combination of Yasukawa/Rhoads/Millsted/Stefik discloses the methods a shown above. Yasukawa/Rhoads/Millsted/Stefik do not disclose:

- *the user-specific authorization information is encrypted,* and
- *an encryption key used to encrypt the user-specific authorization information is at least one of user identification information, equipment identification information loaded in user- employed computers, CPU identification information loaded in*

the user-employed computers, and identification information unique to digital-content-storing recording media.

Applicant, however, on pages 2 and 3 of the specification, discloses encrypting the key using "user-specific identification numbers such as hard disk drive identification numbers." It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Yasukawa/Rhoads/Millsted/Stefik and modify it with the Applicant's use of unique identification numbers because using an ID number that is specific to a computer or a user allows for the generation of a key that can be used only for one person or one machine, thereby making unauthorized use of digital data less likely.

With regard to the limitation of *an encryption key used to encrypt the user-specific authorization information is identification information common to a plurality of users*, applicant inherently discloses common ID numbers. In the case of a client computer on a network, if the user ID were that of a machine part, such as the hard drive or CPU, then the key would be applicable to the machine and any user who has access to the machine. It would have been obvious to one of ordinary skill in the art at the time of the invention to combine Yasukawa/Rhoads/Millsted/Stefik and modify it with the Applicant's use of unique identification numbers common to a group of users because this would simplify the use of digital data where the data is shared by many users on a single machine.

Claim 9:

The combination of Yasukawa/Rhoads/Millsted/Stefik discloses the methods a shown above. Yasukawa/Rhoads/Millsted/Stefik do not disclose that *an encryption key used to encrypt the user-specific authorization information is at least one of identification information unique to distributors of the digital content file, and identification information unique to authors of the digital content file.*. Rhoads, however, in column 40, lines 17-52 discloses using a header to identify the author of a digital work. It would have been obvious to one of ordinary skill in the art at the time

of the invention to combine the encryption method of Yasukawa/Millsted/Stefik/Applicant and modify it with Rhoads' use of header identification because including author identification in the key provides a non-reputable means for identifying the authors of the digital work, thereby preventing unauthorized claims to a digital work.

Claims 10, 11, and 12:

The combination of Yasukawa/Rhoads/Millsted/Stefik discloses the methods a shown above. Yasukawa/Rhoads/Millsted/Stefik do not disclose that *a decryption key for decrypting the encrypted user-specific authorization information is common to an encryption key for encrypting the digital content file, the decryption key being a shared key based on exclusive information transmitted and received among users and content distributors, using symmetric cryptography.* However, Yasukawa discloses that a user "...receives a decryption key which allows decryption and use of the digital information" (column 1, lines 37-38). Yasukawa does not disclose that the keys are generated in pairs. Therefore, Examiner takes **Official Notice** that it is old and well known in the encryption arts to utilize public and private key infrastructure (PKI). Employing PKI establishes a mathematical relationship between implemented between two trusted users on a network, ensuring only authorized use, distribution, and storage of a digital work.

Claims 13, 14, and 15:

The combination of Yasukawa/Rhoads/Millsted/Stefik discloses the methods a shown above. Yasukawa/Rhoads/Millsted/Stefik do not disclose that *digital content file distributors encrypt the encryption key employing a secret key, and the users decrypt the encrypted encryption key employing a public key provided in advance from the digital content file distributors, using public key cryptography.*, Yasukawa discloses that a user "...receives a decryption key which allows decryption and use of the digital information" (column 1, lines 37-38). Yasukawa does not disclose that the keys are generated in pairs. However, Examiner takes

Official Notice that it is old and well known in the encryption arts to utilize public and private key infrastructure (PKI). Employing PKI establishes a mathematical relationship between implemented between two trusted users on a network, ensuring only authorized use, distribution, and storage of a digital work.

Conclusion

9. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

10. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to **James A. Reagan** whose telephone number is **(703) 306-9131**. The examiner can normally be reached on Monday-Friday, 9:30am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, **James Trammell** can be reached at (703) 305-9768.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the **Receptionist** whose telephone number is **(703) 305-3900.** Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://portal.uspto.gov/external/portal/pair . Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to:

(703) 305-7687 [Official communications; including After Final communications labeled "Box AF"]

(703) 308-1396 [Informal/Draft communications, labeled "PROPOSED" or "DRAFT"]

Hand delivered responses should be brought to Crystal Park 5, 2451 Crystal Drive, Arlington, VA, 7th floor receptionist.

JAR

08 March 2005